

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-215029
(P2002-215029A)

(43) 公開日 平成14年7月31日 (2002.7.31)

(51) Int.Cl. ⁷	識別記号	F I	テマコード (参考)
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 D 5 C 0 2 2 6 4 0 B 5 J 1 0 4
H 0 4 L 9/10		H 0 4 N 5/225	F
H 0 4 N 5/225		H 0 4 L 9/00	6 2 1 Z

審査請求 未請求 請求項の数16 O L (全 18 頁)

(21) 出願番号 特願2001-13756(P2001-13756)

(22) 出願日 平成13年1月22日 (2001.1.22)

(71) 出願人 000002369

セイコーエプソン株式会社
東京都新宿区西新宿2丁目4番1号

(72) 発明者 小林 道夫

長野県諏訪市大和3丁目3番5号 セイコーエプソン株式会社内

(72) 発明者 金谷 篤郎

東京都新宿区赤城下町32 カームハイツ1階

(74) 代理人 100066980

弁理士 森 哲也 (外2名)

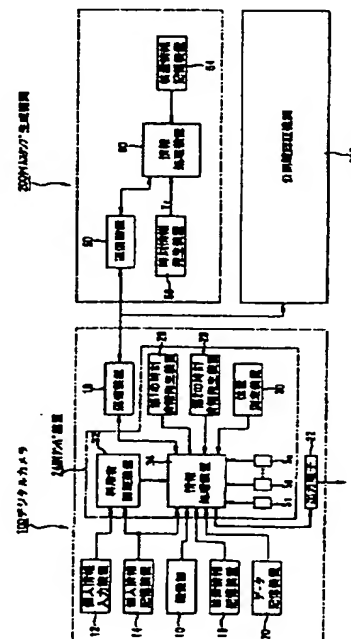
最終頁に続く

(54) 【発明の名称】 情報認証装置及びこれを使用したデジタルカメラ

(57) 【要約】

【課題】 データの客観性を確保することにより、データの証拠としての証明力を向上するのに好適な情報認証装置及びこれを使用したデジタルカメラを提供する。

【解決装置】 デジタルカメラ100は、撮像部10と、情報認証装置としての耐タンバ装置24とで構成されている。耐タンバ装置24は、時刻修正不可能な第1の時刻情報発生装置26、時刻修正可能な第2の時刻情報発生装置28及び位置測定装置30を有し、撮像部10からデジタル画像データが入力されたときに、所有者情報及び位置情報の個別ハッシュ値を算出すると共に、デジタル画像データ、個別ハッシュ値、時刻情報について総合ハッシュ値H_{image}(i)を算出し、さらにデジタル署名S_{image}を算出して記憶すると共に、時刻情報及び位置情報のログ情報を記憶する。



【特許請求の範囲】

【請求項1】 データの認証を行う装置であって、データを入力するデータ入力手段と、前記データ入力手段でデータを入力したことを認証するための複数の認証情報を生成し、これら認証情報のうち選択した認証情報を個別に認証子算出処理して個別認証子を算出すると共に、少なくとも算出した個別認証子入力データについて総合認証識別子を算出する認証識別子算出手段と、該認証識別子算出手段で算出した個別認証識別子及び総合認証識別子を記憶する認証情報記憶手段とを備えていることを特徴とする情報認証装置。

【請求項2】 データの認証を行う装置であって、データを入力するデータ入力手段と、前記データ入力手段でデータを入力したことを認証するための複数の認証情報を生成し、これら認証情報及び前記入力データに前回の総合認証識別子を含めて総合認証識別子を算出する認証識別子算出手段と、該認証識別子算出手段で算出した個別認証識別子及び総合認証識別子を記憶する認証情報記憶手段とを備えていることを特徴とする情報認証装置。

【請求項3】 前記認証識別子算出手段で算出した総合認証識別子に基づいて電子署名を得る電子署名生成手段を有し、前記認証情報記憶手段は、認証識別子算出手段で算出した認証識別子及び前記電子署名生成手段で生成した電子署名を記憶するように構成されていることを特徴とする請求項1又は2に記載の情報認証装置。

【請求項4】 前記電子署名生成手段は、前記認証識別子算出手段で算出した総合認証識別子に基づいて電子署名を得る個別電子署名生成手段と、該個別電子署名生成手段で生成した複数の入力データに対する個別の電子署名を所定数毎に認証識別子算出処理することを繰り返して認証識別子木による総合認証識別子を算出する総合認証識別子算出手段と、該総合認証識別子算出手段で算出した総合認証識別子について電子署名を得る総合電子署名生成手段とを備えていることを特徴とする請求項3に記載の情報認証装置。

【請求項5】 前記電子署名生成手段で生成した電子署名をタイムスタンプ生成機関に送信する送信手段を備えていることを特徴とする請求項3又は4に記載の情報認証装置。

【請求項6】 前記認証識別子算出手段は、認証情報をハッシュ関数処理して算出したハッシュ値を認証識別子として設定するように構成されていることを特徴とする請求項1乃至5の何れかに記載の情報認証装置。

【請求項7】 前記認証識別子算出手段は、使用者による変更が不可能な第1の時間情報発生手段及び使用者による変更が可能な第2の時間情報発生手段を有し、第1及び第2の時間情報発生手段で発生された時間情報を夫々認証情報として設定するように構成されていることを特徴とする請求項1乃至6の何れかに記載の情報認証装置。

【請求項8】 前記認証識別子算出手段は、現在位置を測定する位置測定手段を有し、該位置測定手段で測定した位置に基づいて、前記データ入力手段でデータを入力した地点を特定するための位置情報を生成し、生成した位置情報をハッシュ関数処理してハッシュ値を算出するように構成されていることを特徴とする請求項1乃至7の何れかに記載の情報認証装置。

【請求項9】 前記認証識別子算出手段は、時間情報を発生する時間情報発生手段及び現在位置を測定する位置測定手段を有し、時間情報及び現在位置情報をログ情報として格納することにより、入力データの入力順番、認証装置での入力データの入力を確認可能に構成されていることを特徴とする請求項1乃至6の何れかに記載の情報認証装置。

【請求項10】 前記認証識別子算出手段は、所有者情報を発生する所有者情報入力手段を有し、前記所有者情報入力手段で入力した所有者情報をハッシュ関数処理してハッシュ値を算出し、これを認証情報として入力データに付加するように構成されていることを特徴とする請求項1乃至9の何れかに記載の情報認証装置。

【請求項11】 前記認証識別子算出手段は、物理的なコピー防止機構を有する第1の記憶手段と、該第1の記憶手段と接続されたハッシュ関数演算処理を行う演算処理手段とを有する耐タンパー装置を有し、入力データを物理的なコピー防止機能を持たない第2の記憶手段に格納し、当該入力データを第2の記憶手段に格納する際に、入力データを前記耐タンパー装置の演算処理手段に供給することにより、認証情報と共にハッシュ値を算出し、算出したハッシュ値を第1の記憶手段に記憶するように構成されていることを特徴とする請求項1乃至10の何れかに記載の情報認証装置。

【請求項12】 前記耐タンパー装置は、時間情報をログ情報として第1の記憶手段に記憶するように構成されていることを特徴とする請求項11記載の情報認証装置。

【請求項13】 前記耐タンパー装置は、時間情報及び位置情報をログ情報として第1の記憶手段に記憶するように構成されていることを特徴とする請求項11記載の情報認証装置。

【請求項14】 前記耐タンパー装置は、時間情報、位置情報及び1つ前のエンタリーのハッシュ値をログ情報として第1の記憶手段に記憶するように構成されていることを特徴とする請求項11乃至14の何れかに記載の情報認証装置。

【請求項15】 前記耐タンパー装置は、前記第1の記憶装置の記憶容量に制限がある場合に、記憶すべき情報に電子署名を施して、外部に出力するように構成されていることを特徴とする請求項11乃至14の何れかに記載の情報認証装置。

【請求項16】 デジタル写真データを入力データとす

る請求項1乃至15の何れかに記載の情報認証装置を備えたデジタルカメラ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、データの認証を行う情報認証装置及びこれを使用したデジタルカメラに係り、特に、データの客観性を確保することにより、データの証拠としての証明力を向上することができる情報認証装置及びこれを使用したデジタルカメラに関する。

【0002】

【従来の技術】近年、アメリカ等では、通常のカメラで撮影した写真のほか、デジタルカメラで撮影したデジタル画像も裁判の証拠として認められるようになってきている。しかし、デジタル画像等のデジタルデータは、一般に改竄が比較的容易であるため、証拠の証明力が不十分であるという問題があった。

【0003】従来、デジタルデータの証拠としての証明力を向上する技術に関連するものとして、例えば、特開平11-115831号公報に開示された車両制御イベントデータ認証装置がある。これは、車両事故の発生前、発生中または発生後に運転者によって実行された一連の運転操作等の制御イベントを記録するものであって、制御イベント情報を受信すべく結合され、第1タイム・スタンプおよび車両識別番号VINを制御イベント情報に付加して第1情報を与え、第1情報をタイム・オーバーラップ方式でメモリに出力するマイクロコントローラと、マイクロコントローラおよびマイクロプロセッサに結合され、第1情報および第2情報をタイム・オーバーラップ方式で格納するメモリと、メモリおよび複数のトランスデューサに結合され、受信した衝突データが以前の衝突データとは異なるかどうかを判定し、受信した衝突データが異なるときは、第2タイム・スタンプおよびVINを受信した衝突データに追加して、第2情報を生成するマイクロプロセッサと、で構成されている。

【0004】

【発明が解決しようとする課題】しかしながら、上記従来の車両制御イベントデータ認証装置にあつては、内部タイマから取得した値に基づいてタイム・スタンプを生成してこれを制御イベント情報に付加するようになっているため、内部タイマの値が利用者によって変更されたり、経年劣化等の原因により内部タイマの値がずれたりする可能性があり、制御イベント情報の証拠としての証明力が不十分であるという問題があった。

【0005】また、マイクロコントローラによって記録される制御イベント情報は、マイクロコントローラによって「サイン」が付加される。すなわち、記録された制御イベント情報が特定の車両の運転中に生成されたことを保証するために、タイム・スタンプと所定の識別値とを含むようになっているが、この「サイン」は、内部で独自に生成・付加されるものであるため、客観性に乏し

く、これも証拠としての証明力が不十分である。

【0006】また、パーソナルIDや車両識別番号VINがそのままの状態でもメモリに格納されるため、利用者によって改ざんされる可能性があり、これも証拠としての証明力が不十分である。一方、データの証拠としての証明力を向上する必要性は、裁判だけに限らず、次のような場合にも考えられる。

【0007】例えば、病院等で検査を行う場合には、いつ誰がどこで検査を行ったかということを証明するデータを記録しておくことが考えられるが、こうしたデータは、患者にとって重要なデータであることから、誰にも改ざんされず、客観性を有していることが望まれる。したがって、この場合は、データの証拠としての証明力を向上する必要がある。

【0008】また例えば、宅配便等で荷物を配送する場合には、いつ誰がどのようなルートをとって配送したかを証明するデータを記録しておくことが考えられるが、こうしたデータは、配送過程で荷物が紛失・破損したときに必要なデータであることから、誰にも改ざんされず、客観性を有していることが望まれる。したがって、この場合は、データの証拠としての証明力を向上する必要がある。

【0009】その他の場合としては、事故現場の写真や芸能人のスクープ写真を撮影した場合に撮影者、撮影日または撮影場所を証明するとき、学術調査等で調査データを記録する場合、電話やFAX等で商品またはサービスの注文を受け付けた場合に相手方と注文内容を特定するとき、作曲等をした場合に著作権の発生日を証明するときなどが挙げられる。

【0010】そこで、本発明は、このような従来の技術の有する未解決の課題に着目してなされたものであって、データの客観性を確保することにより、データの証拠としての証明力を向上するのに好適な情報認証装置及びこれを使用したデジタルカメラを提供することを目的としている。

【0011】

【課題を解決するための手段】上記目的を達成するために、本発明に係る請求項1記載の情報認証装置は、データの認証を行う装置であつて、データを入力するデータ入力手段と、前記データ入力手段でデータを入力したことを認証するための複数の認証情報を生成し、これら認証情報のうち選択した認証情報を個別に認証子算出処理して個別認証子を算出すると共に、少なくとも算出した個別認証識別子及び入力データについて総合認証識別子を算出する認証識別子算出手段と、該認証識別子算出手段で算出した個別認証識別子及び総合認証識別子を記憶する認証情報記憶手段とを備えている。

【0012】この請求項1に係る発明では、データ入力手段でデータが入力されると、認証識別子算出手段で、時刻情報、位置情報、所有者情報等の認証情報を生成

し、これら認証情報のうち選択した認証情報例えば位置情報、所有者情報等について個別に認証子算出処理を行ってハッシュ値等の個別認証識別子を算出し、算出した個別認証識別子及び入力データについて総合認証識別子を算出し、これを認証情報記憶手段で記憶する。ここで、認証情報記憶手段は、情報認証装置に内蔵させるようにしてもよく、外部の記憶装置を利用するようにしてもよい。

【0013】また、本発明に係る請求項2記載の情報認証装置は、データの認証を行う装置であって、データを入力するデータ入力手段と、前記データ入力手段でデータを入力したことを認証するための複数の認証情報を生成し、これら認証情報及び前記入力データに前回の総合認証識別子を含めて総合認証識別子を算出する認証識別子算出手段と、該認証識別子算出手段で算出した個別認証識別子及び総合認証識別子を記憶する認証情報記憶手段とを備えていることを特徴としている。

【0014】この請求項2に係る発明では、認証識別子算出手段で、認証情報及び入力データに前回の総合認証識別子を含めて総合認証識別子を生成するので、認証識別子のチェーンを形成することにより、入力データの改竄防止機能をより向上させることができる。さらに、本発明に係る請求項3記載の情報認証装置は、請求項1又は2に係る発明において、前記認証識別子算出手段で算出した総合識別子に基づいて電子署名を得る電子署名生成手段を有し、前記認証情報記憶手段は、認証識別子算出手段で算出した認証識別子及び前記電子署名作成手段で作成した電子署名を記憶するように構成されていることを特徴としている。

【0015】この請求項3に係る発明では、電子署名作成手段で、認証識別子算出手段で算出した総合認証識別子に基づいて電子署名を得るので、電子署名の検証により入力データ及び情報認証装置の特定が可能となる。さらにまた、本発明に係る請求項4記載の情報認証装置は、請求項1乃至3の何れかの発明において、前記電子署名生成手段は、前記認証識別子算出手段で算出した総合認証識別子に基づいて電子署名を得る個別電子署名生成手段と、該個別電子署名生成手段で生成した複数の入力データに対する個別の電子署名を所定数毎に認証識別子算出処理することを繰り返して認証識別子木による総合認証識別子を算出する総合認証識別子算出手段と、該総合認証識別子算出手段で算出した総合認証識別子について電子署名を得る総合電子署名生成手段とを備えていることを特徴としている。

【0016】この請求項4に係る発明では、個別電子署名生成手段で複数の入力データに対して個別に電子署名を生成したときに、これら複数の電子署名を所定数毎にまとめて認証識別子算出処理を行うことを繰り返すことにより、認証識別子木による総合認証識別子を算出し、算出した総合認証識別子について総合電子署名生成手段

で総合電子署名を得るので、この総合電子署名を例えばタイムスタンプ生成機関に送信してタイムスタンプを得ることにより、複数の入力データについて同時にタイムスタンプを得ることができる。

【0017】なおさらに、本発明に係る請求項5記載の情報認証装置は、請求項3又は4の発明において、前記電子署名生成手段で生成した電子署名をタイムスタンプ生成機関に送信する送信手段を備えていることを特徴としている。この請求項5に係る発明では、送信手段で、電子署名生成手段で生成した電子署名を認証局に送信するので、入力データの認証を確実に行うことができる。

【0018】また、本発明に係る請求項6記載の情報認証装置は、請求項1乃至5の何れかの発明において、前記認証識別子算出手段は、認証情報をハッシュ関数処理して算出したハッシュ値を認証識別子として設定するように構成されていることを特徴としている。この請求項6に係る発明においては、認証情報をハッシュ関数処理してハッシュ値を算出するようにしているので、改竄の検出を容易に行うことができると共に、認証情報と入力データとを含む全体のハッシュ関数処理することにより算出した総合ハッシュ値についてタイムスタンプを得るだけで、証拠としての信頼性を確保することができる。

【0019】さらに、本発明に係る請求項7記載の情報認証装置は、請求項1乃至6の何れかの発明において、前記認証識別子算出手段は、使用者による変更が不可能な第1の時間情報発生手段及び使用者による変更が可能な第2の時間情報発生手段を有し、第1及び第2の時間情報発生手段で発生された時間情報を夫々認証情報として設定するように構成されていることを特徴としている。

【0020】この請求項7に係る発明では、時間情報を使用者による変更が不可能な第1の時間情報発生手段及び使用者による変更が可能な第2の時間情報発生手段で個別に発生することにより、両者の時間差から人為的な時刻の改竄を検知することができる。ここで、時間情報発生手段としては、時刻情報を発生する手段の他、使用開始時刻から時間計時を開始するストップウォッチ機構を適用することもでき、ストップウォッチ機構を適用する場合には、使用開始時刻を記憶しておくことにより、時刻換算を行うことができる。

【0021】さらに、本発明に係る請求項8記載の情報認証装置は、請求項1乃至7の何れかの発明において、前記認証識別子算出手段は、現在位置を測定する位置測定手段を有し、該位置測定手段で測定した位置に基づいて、前記データ入力手段でデータを入力した地点を特定するための位置情報を生成し、生成した位置情報をハッシュ関数処理してハッシュ値を算出するように構成されていることを特徴としている。

【0022】この請求項8に係る発明では、例えば全地球測位システム（GPS）等の現在位置測定手段で測定

した現在位置情報を認証情報に含めることができるので、入力データの入力位置を正確に特定することができる。さらにまた、本発明に係る請求項9記載の情報認証装置は、請求項1乃至6の何れかの発明において、前記認証識別子算出手段は、時間情報を発生する時間情報発生手段及び現在位置を測定する位置測定手段を有し、時間情報及び現在位置情報をログ情報として格納することにより、入力データの入力順番、認証装置での入力データの入力を確認可能に構成されていることを特徴としている。

【0023】この請求項9に係る発明では、時間情報及び現在位置情報のログ情報を格納することにより、入力データの入力順番や情報認証装置での入力データの入力を確認することができ、入力データや認証情報の改竄を検知することができる。なおさらに、本発明に係る請求項10記載の情報認証装置は、請求項1乃至9の何れかの発明において、前記認証識別子算出手段は、所有者情報を発生する所有者情報入力手段を有し、前記所有者情報入力手段で入力した所有者情報をハッシュ関数処理してハッシュ値を算出し、これを認証情報として入力データに付加するように構成されていることを特徴としている。

【0024】この請求項10に係る発明では、所有者情報入力手段で、所有者名、入力データがデジタル画像データであるときに撮影データ等のメモ等の所有者情報を入力し、この所有者情報をハッシュ関数処理してハッシュ値を算出するので、検証時に入力データに関する情報を特定することができる。また、本発明に係る請求項11記載の情報認証装置は、請求項1乃至10の何れかの発明において、前記認証識別子算出手段は、物理的なコピー防止機構を有する第1の記憶手段と、該第1の記憶手段と接続されたハッシュ関数演算処理を行う演算処理手段とを有する耐タンパー装置を有し、入力データを物理的なコピー防止機能を持たない第2の記憶手段に格納し、当該入力データを第2の記憶手段に格納する際に、入力データを前記耐タンパー装置の演算処理手段に供給することにより、認証情報と共にハッシュ値を算出し、算出したハッシュ値を第1の記憶手段に記憶するように構成されていることを特徴としている。

【0025】この請求項11に係る発明では、耐タンパー装置で認証情報のハッシュ値を算出すると共に、算出したハッシュ値、他の認証情報及び入力データの全てに対する総合ハッシュ値を算出し、算出したハッシュ値、総合ハッシュ値を物理的なコピー防止機能を持たない第2の記憶手段に記憶することにより、耐タンパー装置内で記憶するハッシュ値が入力データの大きさにかかわらず一定であり、第1の記憶手段の記憶容量を抑制することができる。

【0026】さらに、本発明に係る請求項12記載の情

報認証装置は、請求項11記載の発明において、前記耐タンパー装置は、時間情報をログ情報として第1の記憶手段に記憶するように構成されていることを特徴としている。この請求項12に係る発明では、時間情報をログ情報として第1の記憶装置に記憶するので、このログ情報から入力データの入力順序を特定することができ、特に時間情報として使用者の修正可能な時刻情報及び使用者の修正不可能な時刻情報の2つの時刻情報又は使用者の修正可能な時刻情報及び全地球測位システム（GPS）の時刻情報の2つを使用することにより、時間情報の改竄をより確実に防止する。

【0027】さらにまた、本発明に係る請求項13記載の情報認証装置は、請求項11記載の情報認証装置において、前記耐タンパー装置は、時間情報及び位置情報をログ情報として第1の記憶手段に記憶するように構成されていることを特徴としている。この請求項13に係る発明では、第1の記憶手段に時間情報及び位置情報をログ情報として記憶するので、このログ情報から入力データの入力順序をより確実に特定することができる。

【0028】なおさらに、本発明に係る請求項14記載の情報認証装置は、請求項11記載の発明において、前記耐タンパー装置は、時間情報、位置情報及び1つ前のエントリーのハッシュ値をログ情報として第1の記憶手段に記憶するように構成されていることを特徴としている。この請求項14に係る発明では、請求項12及び13の作用に加えて、1つ前のエントリーのハッシュ値もログ情報として記憶するので、ログ情報のエントリーによるハッシュチェーンを形成することができ、ハッシュチェーンの一方方向性によって少なくともログ情報のエントリーの前後関係を保証することが可能となり、検証時にはエントリーの連続性の検証も行うことから不正なエントリーを隠しこむことを防止することができる。

【0029】また、本発明に係る請求項15記載の情報認証装置は、請求項11乃至14の何れかの発明において、前記耐タンパー装置は、前記第1の記憶装置の記憶容量に制限がある場合に、記憶すべき情報に電子署名を施して、外部に出力するように構成されていることを特徴としている。この請求項15に係る発明では、耐タンパー装置に設ける第1の記憶装置の記憶容量に制限がある場合に、電子署名、タイムスタンプ以外のログ情報、ハッシュ値等の記憶すべき情報に電子署名を施して外部に出力することにより、耐タンパー装置内で生成された正しいものであることを証明することができる。

【0030】さらに、本発明に係る請求項16記載の情報認証装置を使用したデジタルカメラは、デジタル写真データを入力データとする請求項1乃至15の何れかの情報認証装置を備えた構成を有する。このように、デジタルカメラに情報認証装置を設けることにより、撮影したデジタル画像情報の証拠能力を格段に向上させることができる。

【0031】

【発明の実施の形態】以下、本発明の実施の形態を図面について説明する。図1～図5は、本発明に係る情報認証装置をデジタルカメラに適用した場合の一実施形態を示す図である。まず、本発明に係る情報認証装置および認証局を適用する情報認証システムの構成を図1を参照しながら説明する。図1は、情報認証システムの構成を示すブロック図である。

【0032】この情報認証システムは、図1に示すように、情報認証装置を構成するデジタルカメラ100とデジタルデータがある特定時刻に存在していたことを証明するタイムスタンプ生成機関200及びデジタルカメラ100における電子署名を行う際の秘密鍵に対応する公開鍵を登録すると共に、公開鍵に対して電子署名を発行する公開鍵認証機関300とをネットワークを介して通信可能に構成されている。

【0033】デジタルカメラ100は、例えば、通常時はタイムスタンプ生成機関200及び公開鍵認証機関300と接続しておらず、タイムスタンプを得るときにのみタイムスタンプ生成機関200と接続し、同様に公開鍵を登録する際にのみ認証機関300に接続するように構成されている。なお、発明の理解を容易にするため、デジタルカメラ100を1台のみ図示しているが、実際には、異なる複数のデジタルカメラがタイムスタンプ生成機関200及び公開鍵認証機関300と通信可能とされている。

【0034】デジタルカメラ100は、CCD素子等の撮像素子で撮像した画像データをデジタル画像データとして出力するデータ入力手段としての撮像部10と、使用者名、撮影条件（シャッター速度、絞り等）データやメモ等の個人情報を入力する個人情報入力装置12と、入力された個人情報を記憶する個人情報記憶装置14と、デジタルカメラ100に固有の情報である装置情報を記憶する装置情報記憶装置16と、タイムスタンプ生成機関200とネットワークを介して通信する通信装置18と、デジタル画像データを記憶する第2の記憶手段としてのデータ記憶装置20と、デジタルデータを外部に出力するための出力端子22と、デジタルカメラ10でデジタルデータを取り込んだことを認証するための認証識別子を算出する認証識別子算出部としての例えば電源を内蔵するICカードで構成される耐タンパー装置24とを備えている。

【0035】個人情報入力装置12は、入力キーを有し、デジタルカメラ100を利用する各利用者ごとに割り当てられたID、そのIDに対応したパスワード或いは指紋等の個人識別情報、デジタルカメラでの撮影条件やメモ等の所有者情報の入力が可能に構成されている。個人情報記憶装置14は、デジタルカメラ100を利用する各利用者ごとに割り当てられたIDと、そのIDに対応したパスワードと、を暗号化した暗号化個人情報が

格納されている。ここで、ID及びパスワードは、例えば、デジタルカメラの秘密鍵により暗号化されたものである。

【0036】装置情報記憶装置16には、デジタルカメラ100に固有の情報である装置情報（例えば、装置固有の番号）を暗号化した暗号化装置情報が格納されている。ここで、装置情報は、例えば、デジタルカメラの秘密鍵により暗号化されたものである。通信装置18は、近距離無線通信端末、携帯電話やPHS等を利用して、現在地点から最も近くにある基地局を特定し、無線により一般公衆回線網を通じてネットワークに接続し、そのネットワークを介してデジタルデータをタイムスタンプ生成機関200に送信するように構成されている。

【0037】次に、耐タンパー装置24の構成を詳細に説明する。耐タンパー装置24は、時刻を計時して時刻情報を発生する所有者が時刻調整不可能な第1の時間情報発生手段としての第1の時刻情報発生装置26と、時刻を計時して時刻情報を発生する所有者が時刻調整可能な第2の時間情報発生手段としての第2の時刻情報発生装置28と、位置を測定する位置測定手段としての位置測定装置30と、周囲の環境状態を測定する複数のセンサ $S_1 \sim S_n$ と、個人情報入力装置12で入力した個人情報と個人情報記憶装置14の個人情報とを照合して利用者の認証を行う利用者認証装置32と、この利用者認証装置32で正規の利用者であることが認証されたときに、撮像部10、個人情報記憶装置14、装置情報記憶装置16、第1の時刻情報発生装置26、第2の時刻情報発生装置28及び位置測定装置30から入力される入力データを処理する情報処理装置34とで構成されている。

【0038】ここで、耐タンパー装置24は、不活性ガスを封入した気密なパッケージ内に配置され、パッケージを開けると、不活性ガスが飛散して、記憶装置内部が酸化して記憶内容が消失するか又は記憶内容の読出しが不能となるように構成することが記憶情報の改竄を防止する意味で好ましい。位置測定装置30は、衛星からの電波を受信して現在位置を測定する全地球測位システム（GPS）で構成され、緯度情報N及び経度情報Wと衛星時刻情報Tとを情報処理装置34に出力する。

【0039】センサ $S_1 \sim S_n$ は、周囲の環境状態として、例えば、周囲の温度、湿度、気圧、ガス濃度、風速、標高、音量または光量を測定する。これらの物理量を測定するセンサとしては、既知の計測器を用いることができる。利用者認証装置32は、情報処理装置34から利用者の認証要求があったときは、個人情報入力装置12でIDおよび個人識別情報を入力するとともに、個人情報記憶装置14から暗号化個人情報を読み出してこれを復号化し、入力したIDおよび個人識別情報と、復号化したIDおよび個人識別情報とが一致するか否かを判定するように構成されている。判定の結果、これらが

一致すると判定されたときは、正当な利用者であることを示す利用者認証データを情報処理装置34に出力し、これらが一致しないと判定されたときは、不正な利用者であることを示す利用者認証データを情報処理装置34に出力する。

【0040】次に、情報処理装置34の構成を図2を参照しながら説明する。図2は、情報処理装置34の構成を示すブロック図である。情報処理装置34は、図2に示すように、撮像部10から入力されるデジタル画像データ、個人情報記憶装置14に記憶されている所有者情報、装置情報記憶装置16に記憶されている装置情報、第1の時刻情報発生装置26、第2の時刻情報発生装置28で発生される時刻情報及び位置測定装置30から出力される時刻情報及び緯度・経度情報が入力される制御処理部36と、この制御処理部36に入力された情報を認証計算処理としてのハッシュ関数処理を行って認証識別子としてのハッシュ値を算出する演算処理部38と、この演算処理部38の演算結果を記憶すると共に、デジタル署名に必要な秘密鍵及びこれに対する公開鍵を記憶し、さらに演算処理部38で実行する演算処理プログラムを格納した物理的なコピー防止機構を有する記憶装置40とで構成されている。

【0041】そして、演算処理部38では、図3に示す認証識別子演算処理を実行する。この認証識別子演算処理は、デジタルカメラ100で被写体を撮像する撮影モードが設定されたときに実行開始され、まず、ステップS1で、利用者認証装置32に対して利用者の認証要求を出力し、次いでステップS2に移行して、利用者認証装置32から入力された利用者認証データが正当な利用者であることを表すものであるか否かを判定し、不正な利用者であるときにはステップS3に移行して、デジタルカメラ100の電源を強制的に遮断して処理を終了し、正当な利用者であるときにはステップS4に移行する。

【0042】このステップS4では、撮像部10からデジタル画像データが制御処理部36を介して入力されたか否かを判定し、デジタル画像データが入力されていないときにはこれが入力されるまで待機し、デジタル画像データが入力されたときにはステップS5に移行する。このステップS5では、入力されたデジタル画像データ

$$H_{image}(i) = h [Hp1, Hp2, I, t, t', T, E, H_{image}(i-1)]$$

..... (1)

ステップS15では、装置情報記憶装置16から装置情報ID_{camera}を読み込み、次いでステップS16に移行して、総合ハッシュ値H_{image}(i)及び装置情報ID_{camera}に対して記憶装置40に記憶されている秘密鍵を使用してデジタル署名S_{image}(=SIG_{tr}(H_{image}(i), ID_{camera}), tr:耐タンパー装置)を作成してからステップS17に移行して、作成したデジタル署名S_{image}を記憶装置40に記憶してからステップS1

8に必要な応じて暗号化するか署名を付けてデータ記憶部20に記憶し、次いでステップS6に移行して、使用者名UN及び撮影データのメモMMでなる所有者情報を読込んでこれらをデータ記憶装置20に必要な応じて暗号化するかデジタル署名を付けて記憶してからステップS7に移行する。

【0043】このステップS7では、使用者名UN及び撮影条件やメモ等の付加情報MMを所定のハッシュ関数に代入するハッシュ関数処理してハッシュ値Hp1(=h(UN, MM))を算出し、次いでステップS8に移行して算出したハッシュ値Hp1を記憶装置40に記憶してからステップS9に移行する。このステップS9では、位置測定装置30で測定された緯度情報N及び経度情報Wを読み込み、これらをデータ記憶装置20に必要な応じて暗号化するか電子署名を付けて記憶し、次いでステップS10に移行して、緯度情報N及び経度情報Wを所定のハッシュ関数に代入するハッシュ関数処理してこれらのハッシュ値Hp2(=h(N, W))を算出し、次いでステップS11に移行して、算出したハッシュ値Hp2を記憶装置40に記憶してからステップS12に移行する。

【0044】このステップS12では、第1の時刻情報発生装置26、第2の時刻情報発生装置28、位置測定装置30の各時刻情報t, t', T及び環境センサS1~Snで検出した環境状態情報Eを読み込み、少なくとも環境状態情報Eを必要に応じて暗号化するかデジタル署名を付けてデータ記憶装置20に記憶し、次いでステップS13に移行して、ハッシュ値Hp1, Hp2、時刻情報t, t', T、環境状態情報E及び前回の総合ハッシュ値H_{image}(i-1)を認証情報としてデジタル画像データIに付加し、認証情報が付加されたデジタル画像データIについて所定のハッシュ関数に代入するハッシュ関数処理して総合識別子としての下記(1)式で表されるハッシュチェーンを構成する総合ハッシュ値H_{image}(i)を算出し、次いでステップS14に移行して、総合ハッシュ値H_{image}(i)を記憶装置40に記憶してからステップS15に移行する。ここで、認証情報をデジタル画像データIに付加するには、認証情報を電子透かしやサブリミナル情報としてデジタル画像データIに付加する。

8に移行する。

【0045】このステップS18では、前記ステップS12で読込んだ第1の時刻情報発生装置26で発生された時刻情報t、第2の時刻情報発生装置28で発生された時刻情報t'及び位置測定装置30の時刻情報TとステップS9で読込んだ緯度情報N及び経度情報Wとをログ情報として記憶装置40のログ情報記憶領域に記憶してからステップS19に移行する。

【0046】このステップS19では、タイムスタンプ生成機関200に対してタイムスタンプを要求するか否かを判定し、タイムスタンプを要求しないときには後述するステップS23にジャンプし、タイムスタンプを要求するときにはステップS20に移行し、ステップS17で記憶したデジタル署名 S_{image} を通信装置18を介してタイムスタンプ生成機関200に送信してからステップS21に移行する。

【0047】このステップS21では、タイムスタンプ生成機関200からタイムスタンプ S_{IGTSA} (S_{image} , T_T)を受信したか否かを判定し、タイムスタンプを受信していないときにはこれを受信するまで待機し、タイムスタンプを受信したときにはステップS22に移行して、受信したタイムスタンプ S_{IGTSA} (S_{image} , T_T)を記憶装置40に記憶してからステップS23に移行し、デジタルカメラの撮影モードが終了したか否かを判定し、撮影モードが継続されているときには前記ステップS1に戻り、撮影モードが終了したときには認証識別子演算処理を終了する。

【0048】この図3の処理において、ステップS1～S23の処理が認証識別子算出手段に対応し、このうちステップS16の処理が電子署名生成手段に対応し、ステップS19及びS20の処理と送信装置18とが送信手段に対応している。また、演算処理部38では、デジタル画像データの出力要求があったときに、データ記憶装置20に記憶されているデジタル画像データと情報処理装置34の記憶装置40に記憶されているハッシュ値 H_{p1} 、 H_{p2} 又はこれらのもとなるデータ、時刻情報 t 、 t' 、 T 、環境情報 E 、総合ハッシュ値 $H_{image(i)}$ 、デジタル署名 S_{image} 、タイムスタンプ S_{IGTSA} ($H_{image(i)}$), T_T)を出力端子22に出力する。

【0049】次に、図1に戻り、タイムスタンプ生成機関200の構成を説明する。タイムスタンプ生成機関200は、図1に示すように、デジタルカメラ100とネットワークを介して通信する通信装置50と、正確な時刻情報 T_T を発生する時刻情報発生装置52と、通信装置50でデジタルカメラ100からデジタル署名 S_{image} を受信すると、その受信した時点の時刻情報 T_T を時刻情報発生装置52から取得し、デジタル署名 S_{image} 及び時刻情報 T_T に対してタイムスタンプ生成機関200の秘密鍵を使用してデジタル署名 S_{IGTSA} (S_{image} , T_T)をタイムスタンプとして生成し、生成したタイムスタンプ S_{IGTSA} (S_{image} , T_T)を自己のデータベースに装置情報 ID_{camera} をインデックスとして登録する。或いはハッシュチェーンに組み込むと共に、定期的にハッシュチェーンの値を例えば新聞等に公開する。そして、タイムスタンプ S_{IGTSA} (S_{image} , T_T)をデジタルカメラ100に送信する。

【0050】ここで、デジタルカメラ100及びタイムスタンプ生成機関200との間でのデータ通信は、公開鍵暗号化方法を使用して、個々の秘密鍵で送信データを暗号化して送信し、受信側で公開鍵を使用して受信データを復号化することが好ましい。次に、上記実施形態の動作を説明する。

【0051】デジタルカメラ100を販売する際に、耐タンパー装置24と、署名検証用の公開鍵とをセットで販売する。デジタルカメラ100を購入した所有者は、証拠能力を必要とするデジタル画像データを撮像する場合に、デジタルカメラ100に耐タンパー装置24を装着して、被写体を撮像する。利用者は、耐タンパー装置24を装着したデジタルカメラ100でデジタル画像を取り込むには、まず、デジタルカメラ100に電源を投入し、IDおよび個人識別情報を個人情報入力装置12から入力する。

【0052】ここで、利用者が正当なID及び個人識別情報を入力したものとすると、耐タンパー装置24では、利用者認証装置32により、個人情報記憶装置14から暗号化個人情報が読み出されてこれが復号化され、個人情報入力装置12から入力されたIDおよび個人識別情報と、復号化されたIDおよび個人識別情報と、が一致するので、正当な利用者であることを示す利用者認証データが情報処理装置34に出力される。情報処理装置34では、正当な利用者であることを示す利用者認証データが入力されると、ステップS1、S2を経て、正当な利用者であると認証され、撮像部10でデジタル画像を取り込み可能な状態となる。

【0053】この状態で、利用者が撮像部10でデジタル画像を取り込むと、情報処理装置34では、撮像部10からデジタル画像データが入力されるので、デジタル画像データをデータ記憶装置20に記憶し(ステップS5)、次いで、個人情報入力装置12で入力された使用者名 UN 、撮影条件等のメモ MM 等の所有者情報をデータ記憶装置20に暗号化して又はデジタル署名を付けて記憶すると共に、所有者情報を所定のハッシュ関数に代入してハッシュ値 H_{p1} を算出し(ステップS7)、算出したハッシュ値 H_{p1} を記憶装置40に記憶する(ステップS8)。

【0054】次いで、位置測定装置30で測定した現在位置を表す緯度情報 N 及び経度情報 W を読み込み(ステップS9)、次いで読込んだ緯度情報 N 及び経度情報 W を所定のハッシュ関数に代入してハッシュ値 H_{p2} を算出し(ステップS10)、算出したハッシュ値 H_{p2} を記憶装置40に記憶する(ステップS11)。次いで、第1の時刻情報発生装置26、第2の時刻情報発生装置28及び位置測定装置30から時刻情報 t 、 t' 及び T を読み込むと共に、センサ $S_1 \sim S_n$ で測定した例えば、周囲の温度、湿度、気圧、ガス濃度、風速、標高、音量または光量でなる環境状態情報 E を読み込み、少なくとも環境情

報Eをデータ記憶装置20に暗号化して又はデジタル署名を付けて記憶し(ステップS12)、デジタル画像データ1にハッシュ値Hp1、Hp2、時刻情報t、t'、T、環境状態情報E及び前回の総合ハッシュ値Himage(i-1)を付加して所定のハッシュ関数に代入することにより総合ハッシュ値Himage(i)を算出し(ステップS13)、算出した総合ハッシュ値Himage(i)を記憶装置40に記憶する(ステップS14)。

【0055】このように、総合ハッシュ値Himage(i)を算出する際に、前回のデジタル画像取込時に算出した総合ハッシュ値Himage(i-1)を付加してハッシュ値を算出することにより、デジタルカメラ100の撮像部10で撮像したデジタル画像データの撮像順序に応じたハッシュチェーンを構成するので、後述するように所望のデジタル画像データの撮影時点でタイムスタンプ生成機関200に対してタイムスタンプを要求することにより、それ以前のデジタル画像データを他のデジタル画像データに置き換えることは不可能となる。

【0056】また、所有者情報及び撮影位置情報について個別にハッシュ値Hp1及びHp2を算出するようにしているので、デジタル署名検証時にハッシュ値Hp1及びHp2毎に個別に情報開示可能となる即ち両情報を公開したくないときにはハッシュ値Hp1又はHp2を公開するのみとし、所有者情報及び撮影位置情報の一方を公開する場合には、所有者情報及び撮影位置情報の一方を公開し、他方をハッシュ値で公開する。ここで、所有者情報としては、撮影条件を個々に公開する場合には、これらの夫々についてハッシュ値を算出して、これらを記憶しておくことが望ましい。

【0057】次いで、総合ハッシュ値Himage(i)と装置情報IDcameraとについて記憶装置40に格納されている秘密鍵を使用してデジタル署名Simageを生成し(ステップS16)、生成したデジタル署名Simageを記憶装置40に記憶する(ステップS17)。その後、第1の時刻情報発生装置26で発生される時刻情報t、第2の時刻情報発生装置28で発生される時刻情報t'及び位置測定装置30の時刻情報Tと、位置測定装置30で測定した緯度情報N及び経度情報Wとをログ情報として記憶装置40に記憶する。

【0058】このため、記憶装置40に記憶されているログ情報に基づいて外部との相互作用が全くない状況においても、耐タンパー性を保証できる限り時刻情報に信頼を寄せることができる。すなわち、第1の時刻発生装置26は使用者による修正が不能に構成されているので、仮に時刻精度が悪いものとしても、事後に正確な時刻に対する遅延時間又は進み時間がある程度推定可能であり、この第1の時刻発生装置28で発生された時刻情報tに基づいて法廷などで人為的な時刻の操作を発見することが可能となる。

【0059】その後、ステップS19でタイムスタンプ

要求を行うか否かを判定し、タイムスタンプ要求を行わないときには、直接ステップS23に移行して、撮影モードを終了したか否かを判定し、撮影モードが継続されているときには前記ステップS4に戻り、撮影モードが終了されたときには認証識別子演算処理を終了する。一方、ステップS19の判定結果がタイムスタンプ要求を行う場合には、記憶装置40に記憶されている装置情報IDcameraと今回のデジタル署名Simageとを耐タンパー装置24の記憶装置40に暗号化して記憶されている秘密鍵を使用して暗号化し、暗号化されたデジタル署名Simageを送信元アドレスをデジタルカメラ100の固有アドレスとし、送信先アドレスをタイムスタンプ生成機関200のアドレスとする送信パケットに付加して通信装置18を介してタイムスタンプ生成機関200に送信する。

【0060】タイムスタンプ生成機関200では、暗号化された装置情報IDcamera及びデジタル署名Simageを受信すると、送信元アドレスから送信元を特定し、登録されているデジタルカメラ100であるか否かを判定し、登録されているデジタルカメラ100であるときに、デジタルカメラ100の公開鍵を選択し、選択した公開鍵を使用して、装置情報IDcamera及びデジタル署名Simageを復号し、装置情報IDcameraが装置情報記憶装置54に記憶されている装置情報IDcameraと一致するか否かを判定し、両者が一致するときに、デジタル署名Simageと時刻情報発生装置56で発生される時刻情報TTとをタイムスタンプ生成機関200の秘密鍵を使用してデジタル署名SIGTSA(Simage, TT)をタイムスタンプとして生成し、生成したタイムスタンプSIGTSA(Simage, TT)を装置情報IDcameraをインデックスとして自己のデータベースに登録すると共に、通信装置50を介してデジタルカメラ100に送信する。

【0061】デジタルカメラ100では、タイムスタンプ生成機関200からタイムスタンプSIGTSA(Simage, TT)を受信すると、これを耐タンパー装置24の情報処理装置34における記憶装置40に記憶する。このようにして、デジタルカメラ100のデータ記憶装置20に撮像したデジタル画像データが順次記憶されると共に、各デジタル画像データに対応する個別ハッシュ値Hp1、Hp2、総合ハッシュ値Himage(i)、デジタル署名Simage(=SIGtr(Himage(i), IDcamera))及びタイムスタンプSIGTSA(Simage, TT)が耐タンパー装置24の記憶装置40に記憶される。

【0062】そして、デジタルカメラ100を撮影モードから再生モードとすると、データ記憶装置20に記憶されているデジタル画像データを液晶ディスプレイ(図示せず)に出力して、この液晶ディスプレイにデジタル画像データを表示する。また、この再生モードからデー

タ出力モードとすると、データ記憶装置20に記憶されているデジタル画像データに、このデジタル画像データに対応する個別ハッシュ値Hp1、Hp2、総合ハッシュ値Himage(i)、デジタル署名Simage(=SIGtr(Himage(i), IDcamera)、タイムスタンプを得ている場合にはタイムスタンプSIGTSA(Simage, Tt)を含む認証情報を付加して、先頭のデジタル画像情報から順次出力端子22へ出力することができ、これら出力データをフラッシュメモリ等の記憶媒体に直接記憶するか又はパーソナルコンピュータ等の情報処理装置に読込んでハードディスク、光磁気ディスク等の記憶媒体に記憶することができる。

【0063】このように、デジタルカメラ100で被写体を撮像して、デジタル画像データをデータ記憶装置20に記憶すると共に、認証情報を耐タンパー装置24の記憶装置40に記憶しておくことにより、法廷等でデジタル画像データを証拠として提出する場合には、デジタルカメラ100でデータ出力モードを選択して、データ記憶装置20及び耐タンパー装置24の記憶装置40に記憶されているデジタル画像データ及び個別ハッシュ値Hp1、Hp2、総合ハッシュ値Himage(i)、デジタル署名Simage(=SIGtr(Himage(i), IDcamera)、タイムスタンプを得ている場合にはタイムスタンプSIGTSA(Simage, Tt)を含む認証情報を順次読出して出力端子22から所定の検証装置に出力する。

【0064】この検証装置では、入力されるデジタル画像データ及び認証情報に基づいてデジタル画像データの検証を行う。すなわち、デジタル署名Simage(=SIGtr(Himage(i), IDcamera)を検証することにより、耐タンパー装置24の特定が可能であり、デジタルカメラ100の特定が可能となる。

【0065】また、総合ハッシュ値Himage(i)が前回の総合ハッシュ値Himage(i-1)を含むハッシュチェーンとして生成されているので、全てのデジタル画像データに対してタイムスタンプを要求する必要がなく、ある時点で総合ハッシュ値Himage(i)のデジタル署名Simageをタイムスタンプ生成機関200に送信してタイムスタンプSIGTSA(Simage, Tt)を得ることにより、それ以前のデジタル画像データや認証情報を改竄することが不可能となり、より大きな改竄防止効果を発揮することができる。

【0066】さらに、撮像時刻については、位置測定装置30で全地球測位システム(GPS)から時刻情報Tを得ている場合には、この時刻情報Tで正確な時刻証明が可能であり、位置測定装置30で衛星からの電波を受信できず、時刻情報Tが得られない場合には、使用者が時刻修正不能な第1の時刻情報発生装置26で発生される時刻情報t及び使用者が正確な時刻に修正した第2の時刻情報発生装置28で発生される時刻情報t'が少な

くとも記憶されているので、第2の時刻情報発生装置28で発生される正確な時刻情報t'によって時刻証明が可能となる。このとき、時刻情報t'と時刻修正不能な第1の時刻情報発生装置26で発生される時刻情報tとの偏差が予め予測される誤差の範囲内であるときに、時刻情報t'が正確な時刻であると認定することができる。この時刻の検証では、タイムスタンプ機関200でのタイムスタンプSIGTSA(Simage, Tt)を得ている場合には、より確実な検証を行うことができる。

【0067】さらにまた、撮影場所については、個別ハッシュ値Hp1、Hp2や、総合ハッシュ値Himage(i)に緯度情報N及び経度情報Wが含まれているので、これらを検証することにより、緯度及び経度を特定することができ、撮影場所の特定が可能となる。このように、総合ハッシュ値Himage(i)の他に個別ハッシュ値Hp1、Hp2を用いることにより、裁判等の際に署名の検証を行う場合に、一部のデータを公表しなければならない時にも他のデータを隠しておくことが可能となる。すなわち、例えばデジタル画像データの撮影場所を署名の検証によって証明しなくてはならない場合、生のデータで公表が必要なのは位置情報N、Wだけになる。すなわち、デジタル署名Simageは[Hp1, Hp2, l, t, t', T, E, Himage(i-1)]と位置情報N、Wと公開鍵があれば検証可能であり、デジタル署名やハッシュ関数の一方向性により位置情報N、Wがデジタル署名Simageの算出に用いられていることが証明できる。

【0068】しかも、総合ハッシュ値Himage(i)には前回の撮像時の総合ハッシュ値Himage(i-1)を含めてハッシュ値を算出することによりハッシュチェーンが構成されるので、総合ハッシュ値Himage(i)を生成後にデジタル画像データの改竄を行うことは不可能となる。なおさらに、デジタルカメラ100を不正に使用する場合には、所有者のID及び個人識別情報を個人情報入力装置12から正確に入力することができないので、図3の認証識別子演算処理のステップS2からステップS3に移行して強制的にデジタルカメラ100の電源が遮断されることになり、所有者以外の不正使用者の使用を禁止することができる。

【0069】また、デジタルカメラ100を不正に取得した不正使用者が耐タンパー装置24を取り外した場合には、撮像部10で撮像した被写体のデジタル画像データをデータ記憶装置20に格納することはできるが、ハッシュ値等の認証情報を生成してタイムスタンプ生成機関200に送信することができず、撮像したデジタル画像データを証明することはできない。但し、撮影したデジタル画像データのハッシュ値を生成してこれをタイムスタンプ生成機関200に送信して、タイムスタンプを得ることにより、その時点でデジタル画像データが存在していたことは保証することができる。

【0070】このように、デジタルカメラ100から耐

タンパー装置24が取り外された場合でも、耐タンパー性が破られる以前にタイムスタンプが発行された事実があればタイムスタンプ生成機関200のデータベースに格納されている装置情報ID_{camera}から撮影したデジタルカメラ100を証明することができる。さらに、デジタルカメラ100を不正に取得した不正使用者が耐タンパー装置24を破壊して、記憶装置40を取り出して、秘密鍵及びハッシュ関数演算やデジタル署名のアルゴリズムを盗もうとした場合には、耐タンパー装置24のパッケージを破った時点で、不活性ガスが外部に流出することにより、記憶装置40が酸化して、記憶装置40の記憶内容が消失することにより、秘密鍵及びハッシュ関数演算やデジタル署名のアルゴリズムを不正取得することを確実に防止することができる。

【0071】さらにまた、デジタルカメラ100が盗まれた場合には、正規の所有者が公開鍵認証機関300に盗難を通知することにより、公開鍵に対するデジタル署名の付加を停止することにより、公開鍵の妥当性が認められなくなり、不正使用者がデジタルカメラ100のID及び個人識別情報を解析するか不正に取得することにより、図3の認証識別子演算処理を実行して個別ハッシュ値Hp1、Hp2、総合ハッシュ値H_{image}(i)、デジタル署名S_{image}及びタイムスタンプを不正に得た場合でも、その後の公開鍵に公開鍵認証機関300のデジタル署名が付加されることはないので、デジタルカメラ100の認証ができなくなり、どのデジタルカメラで撮ったデジタル画像データであるかを証明することができない。

【0072】なおさらに、デジタルカメラ100の撮像部10で被写体を撮像して、デジタル画像データを情報処理装置34に入力したときに、建物内等で位置測定装置30で衛星からの電波を受信することができず、緯度情報N、経度情報W及び時刻情報Tを出力できないときには、総合ハッシュ値H_{image}(i)を生成する際に、これら緯度情報N、経度情報W及び時刻情報Tのフィールドに値が入らない状態となり、撮影位置の特定はできなくなる。

【0073】しかしながら、その前後の何れかで短い時間内に撮像部10で撮像してデジタル画像データを入力したときに、位置測定装置30から緯度情報N、経度情報W及び時刻情報Tが入力されているときには、これらの情報から位置情報を予測することができる。また、時刻情報Tについては、前述したように第1の時刻情報発生装置26及び第2の時刻情報発生装置28で時刻情報t及びt'が発生されており、これらを含んで総合ハッシュ値H_{image}(i)が生成されることにより、時刻の特定を行うことができる。

【0074】また、衛星からの電波を受信できない建物内等で、使用者が故意に、不正な時刻を載せた衛星からの電波と同じ電波をデジタルカメラ100に与えること

により、位置測定装置30から不正な緯度情報N、経度情報W及び時刻情報Tを出力するようにした場合には、耐タンパー装置24で第1の時刻情報発生装置26及び第2の時刻情報発生装置28で発生される時刻情報t、t'及びTと緯度情報N及び経度情報Wとのログ情報を記憶装置40に記憶しているので、このログ情報を解析することにより、時刻情報Tと緯度情報N及び経度情報Wの恣意的な狂いを発見することができ、不正を正確に検出することができる。

【0075】すなわち、ログ情報が下表1に示すように、第1の時刻情報発生装置26で発生された使用者に修正不可能な時刻情報tと位置測定装置30で測定して全地球測位システム(GPS)による時刻情報Tである場合に、最初に撮影してデジタル画像データを入力したエントリーAについては修正不可能な時刻情報tが12:05:00であり、且つ時刻情報Tが12:00:00であり、これに続くエントリーBについては時刻情報tが12:06:00であり、時刻情報Tについては衛星からの電波を受信できずに空きフィールドとなり、その後のエントリーCについては時刻情報tが12:07:00であり、時刻情報Tが12:01:58であるときには、時刻情報tに基づいてエントリーBの空きフィールドはエントリーA及びエントリーCの時刻情報Tの平均であることが予測され、12:00:59であることが推測される。

【0076】

【表1】

	修正不可能 時刻情報t	GPS 時刻情報T
A	12:05:00	12:00:00
B	12:06:00	空
C	12:07:00	12:01:58

【0077】さらに、ログ情報として時刻情報、緯度情報N、経度情報W及び1つ前のデジタル画像データエントリー時の総合ハッシュ値H_{image}(i)も記録して、ログ情報でもエントリーによるハッシュチェーンを形成すると、ハッシュチェーンの一方方向性によって少なくともログ情報のエントリーの前後関係は保証させることになる。また、検証時にはエントリーの連続性の検証も行わなければならないことから、使用者は不正なエントリーを隠すことができなくなり、改竄の防止効果をより確実に発揮することができる。

【0078】さらにまた、修正可能な時刻情報t'については所有者が手動で修正してもよいし、位置測定装置30からの時刻情報T又は時刻電波を受信したときに、受信した時刻情報Tに応じて自動修正するようにしてもよい。なお、上記実施形態においては、耐タンパー装置24をパッケージを開けたときに酸化によって記憶装置40の記憶内容が消失するようにした場合について説明

したが、これに限定されるものではなく、情報処理装置34に不正アクセスしてプログラムを解析しようとしたときに、情報処理装置34で不正アクセスを自動検知して記憶装置40に格納されているプログラム、秘密鍵、認証情報を自動的に消去するようにしてもよく、或いはパッケージに各種センサを配置して、パッケージが開かれることを検出したときに記憶装置40に格納されているプログラム、秘密鍵、認証情報を自動的に消去するようにしてもよい。

【0079】また、上記実施形態においては、耐タンパー装置24に設けた記憶装置40にハッシュ値、デジタル署名、タイムスタンプ、ログ情報等を記憶するようにした場合について説明したが、これに限定されるものではなく、耐タンパー装置24を小型化する場合には、ハッシュ値、デジタル署名、タイムスタンプ及びログ情報を必要に応じて暗号化するかデジタル署名を付けて外部のデータ記憶装置20に記憶し、記憶装置40として秘密鍵や処理プログラム等の必要最小限の情報を記憶するROM構成とするようにしてもよい。この場合、外部に記憶するハッシュ値、ログ情報等には認証性を向上させるためにデジタル署名をつけて記憶することが好ましい。

【0080】さらに、上記実施形態では、総合ハッシュ値 $H_{\text{image}}(i)$ の算出時に1つ前のエントリー時の総合ハッシュ値 $H_{\text{image}}(i-1)$ を付加する場合について説明したが、これに限定されるものではなく、ハッシュチェーンの作成を行わないようにしてもよい、この場合には、ハッシュチェーンによる検証が不能であることから、複数のデジタル画像データの撮影毎に、又は撮影終了後にまとめて個々のデジタル画像データ毎にタイムスタンプを要求する必要がある。

【0081】この場合には、個々のデジタル画像データ毎にタイムスタンプを要求するのは非現実的である。そこで、タイムスタンプを要求したい複数例えば8個のデジタル画像データについて個別電子署名生成手段で個別デジタル署名 S_j ($j=1, 2, \dots, 8$)を生成し、これら個別デジタル署名 S_j に基づいて以下のようなハッシュ（認証識別子）木を構成する。

【0082】 $H_j = h(S_j)$ ($j=1, \dots, 8$)
 $H_A = h(H_1, H_2)$, $H_B = h(H_3, H_4)$,
 $H_C = h(H_5, H_6)$, $H_D = h(H_7, H_8)$
 $H_\alpha = h(H_A, H_B)$, $H_\beta = h(H_C, H_D)$
 $H_{\text{ALL}} = h(H_\alpha, H_\beta)$

その上で、さらに総合ハッシュ値 H_{ALL} に総合電子署名手段でデジタル署名を施し、このデジタル署名に対するタイムスタンプを要求する。この操作により夫々に対して厳密ではないが8つの全てのデジタル署名 S_j に対して同時にタイムスタンプが発行されることになり、これらのデジタル画像データの信憑性を与えることができる。

【0083】このように、ハッシュ木を採用する場合には、例えば上記のような2分木ハッシュである場合には、 2^N 個のデジタル画像データがある場合のうちの1枚の撮影順序等を証明する場合、該当するデジタル画像データと総合ハッシュ値 H_{ALL} の他 N 個のハッシュ値を記憶しておけばよく、記憶データ数を大幅に減少させることができる。

【0084】すなわち、図4に示すように、16(24)個のデジタル画像データ $D_1 \sim D_{16}$ が存在する場合に、1つのデジタル画像データ D_4 のみを証拠データとして保存したい場合には、このデジタル画像データ D_4 、総合ハッシュ値 H_{ALL} の他、デジタル画像データ D_4 と対となるデジタル画像データ D_5 のハッシュ値 h_5 、その上位における相手側のハッシュ値 h_a 、さらに上位における相手側のハッシュ値 h_b 、さらに上位における相手側のハッシュ値 h_c の計4つハッシュ値を記憶しておけば、デジタル画像データ D_4 の証明が可能となる。なお、デジタル画像データ数が 2^N 個ではないときには、 2^N 個となるようにダミーデータを挿入してハッシュ値計算を行うようにすればよい。

【0085】さらにまた、上記実施形態においては、タイムスタンプ生成機関200で利用者のハッシュ値や時刻情報に対するデジタル署名を生成して、そのデジタル署名をタイムスタンプとするシンプルプロトコル(Simple Protocol)方式を採用する場合について説明したが、これに限定されるものではなく、複数の利用者のハッシュ値を相互に関連づけるリンク情報を生成し、各タイムスタンプがそれまでに生成された全てのタイムスタンプに遺贈するように生成されるリンキングプロトコル(Linking Protocol)方式や、ある時刻のリンク情報を、その時刻に送付されたハッシュ値やその直前のリンク情報から生成し、このリンク情報を定期的に新聞等に公表するようにしたリニアリンキングプロトコル(Linear Linking Protocol)方式等の任意のプロトコルを採用することができる。

【0086】なおさらに、上記実施形態においては、タイムスタンプ生成機関200で時刻情報発生装置56で発生した時刻情報をタイムスタンプに含めるようにした場合について説明したが、これに限定されるものではなく、時刻情報を含まない形式のタイムスタンプを発行するようにしてもよい。また、上記実施形態においては、全地球測位システム(GPS)を利用して位置情報を得る場合について説明したが、これに限定されるものではなく、時報電波を受信する時報電波受信機能を設け、時報電波を受信することにより、時刻情報を得るようにしてもよく、さらには携帯電話機能やPHS機能を付加して、これら携帯電話機能やPHS機能で通信可能な地上局の位置情報入手するようにしてもよく、これら携帯電話機能やPHS機能を全地球測位システムで位置測定

不能時に使用するようにしてもよい。この場合、位置情報を送出する地上局等でデジタル署名付きの位置情報データを送出することにより、より認証機能を向上させることができる。

【0087】さらに、上記実施形態においては、本発明をデジタルカメラに適用した場合について説明したが、これに限定されるものではなく、他の認証を必要とするデジタルデータを出力するパーソナルコンピュータ、CAD等の任意の情報処理装置に本発明を適用することができる。さらにまた、上記実施形態においては、総合ハッシュ値 $H_{image}(i)$ の算出時にハッシュ値を算出しない時刻情報 t, t', T 及び、環境情報 E を含めてハッシュ値を算出する場合について説明したが、これに限定されるものではなく、時刻情報 t, t' 及び T 、環境情報 E についてもハッシュ値を算出してから総合ハッシュ値 $H_{image}(i)$ を算出するようにしてもよく、この場合には時刻情報 t, t' 及び T や環境情報 E について公開したくないときにハッシュ値を公開するのみで実際の情報を公開しないでも済むという利点がある。さらにはハッシュ値を算出しない時刻情報 t, t', T 及び、環境情報 E についてはデジタル署名 S_{image} を作成する時点で下記のように総合ハッシュ値 $H_{image}(i)$ に付加するようにしてもよい。

【0088】 $S_{image} = S_{IGtr}(H_{image}(i), t, t', T, E)$

なおさらに、上記実施形態においては、デジタルカメラ100を購入した直後に公開鍵を公開鍵認証機関300に登録する場合について説明したが、これに限定されるものではなく、所望の時点で公開鍵に登録すれば、その時点から後に撮影したデジタル画像データに対して証明が可能であり、それより以前のデジタル画像データに関しても耐タンパー装置24内の秘密鍵でデジタル署名 S_{image} が生成されていればデジタルカメラ100で撮影したことを証明することができる。

【0089】また、上記実施形態においては、耐タンパー装置24に2つの時刻情報発生装置26及び28を設けた場合について説明したが、これに限定されるものではなく、使用者の修正が不可能な第1の時刻情報発生装置26としては、時刻情報を発生する場合に代えて、使用開始時点からの時間を計時するストップウォッチ機構に置換したり、或いは所定間隔のクロックパルスをカウントするソフトウェアカウンタ機能を持たせるようにしてもよく、使用開始時点を記憶しておけば、時刻情報を換算することができる。

【0090】さらに、上記実施形態においては、認証識別子としてハッシュ関数演算によるハッシュ値を適用した場合について説明したが、これに限定されるものではなく、他のハッシュ値に同等の値が得られる関数演算により認証識別子を演算するようにしてもよく、さらにはハッシュ値に秘密鍵（共通鍵）の署名をつける所謂MA

C (Message Authentication Code)、ハッシュ値に公開鍵の署名を付けたデジタル署名、さらにはハッシュ関数を利用することなく、データ全体を公開鍵で署名した所謂メッセージリカバリー型のデジタル署名等の認証子を適用することができる。

【0091】さらにまた、上記実施形態においては、デジタルカメラ100で撮影したデジタル画像データ及びこれに関する個人情報、位置情報等を耐タンパー装置24で認証する場合について説明したが、これに限定されるものではなく、デジタルカメラ100に装着するフラッシュメモリ等の記憶媒体やUSBケーブル等の接続ケーブルを介して入力されたデジタル画像データについて耐タンパー装置24でデジタル署名を付けることもできる。この場合、デジタルカメラ100で直接撮影したデジタル画像データと外部から入力したデジタル画像データを区別する必要があり、両者の区別は環境変数 E にデジタルカメラ100自身で撮影したデジタル画像データであるか外部から読込んだデジタル画像データであるかを判別するデータ種別情報を自動的に又は手動で付加することにより可能となる。

【0092】そして、外部読込デジタル画像データに対してデジタル署名を付ける場合には、外部読込デジタル画像データを読込んだ使用者の個人の署名鍵を耐タンパー装置24に読込み、その個人署名鍵のみを利用してデジタル署名するようにし、デジタルカメラ100の秘密鍵によるデジタル署名を避けて、デジタルカメラ100で撮影したデジタル画像データの偽造を防止することが望ましい。

【0093】このとき、個人の署名鍵の読込みは、ICカードで構成されるIDカードに個人の署名鍵を記憶させておき、このIDカードをデジタルカメラ100に設けたICカードリーダーで読込むか、個人の署名鍵を記憶した記憶媒体から署名鍵を読出すようにしてもよい。

【0094】

【発明の効果】以上説明したように、請求項1に係る発明によれば、データ入力手段でデータが入力されると、認証識別子算出手段で、時刻情報、位置情報、所有者情報等の認証情報を生成し、これら認証情報のうち選択した認証情報例えば位置情報、所有者情報等について個別に認証子算出処理を行ってハッシュ値等の個別認証識別子を算出し、少なくとも算出した個別認証識別子及び入力データについて総合認証識別子を算出し、これを認証情報記憶手段で記憶するので、個別認証識別子を算出した認証情報について検証時に個別認証識別子の認証情報を個別に開示することが可能となるという効果が得られる。

【0095】また、請求項2に係る発明によれば、認証識別子算出手段で、認証情報及び入力データに前回の総合認証識別子を含めて総合認証識別子を生成するので、認証識別子のチェーンを形成することにより、入力デー

タの改竄防止機能をより向上させることができると共に、タイムスタンプを得る場合に常時タイムスタンプを得る必要がなく、所望時にタイムスタンプを得れば、それ以前の入力データの改竄が不可能となるという効果が得られる。

【0096】さらに、請求項3に係る発明によれば、デジタル署名作成手段で、認証識別子算出手段で算出した総合認証識別子に基づいてデジタル署名を得るので、デジタル署名の検証により入力データ及び情報認証装置の特定が可能となるという効果が得られる。さらにまた、請求項4に係る発明によれば、個別デジタル署名生成手段で複数の入力データに対して個別に電子署名を生成したときに、これら複数の電子署名を所定数毎にまとめて認証識別子算出処理を行うことを繰り返すことにより、認証識別子木による総合認証識別子を算出し、算出した総合認証識別子について総合電子署名生成手段で総合電子署名を得るので、この総合電子署名を例えばタイムスタンプ生成機関に送信してタイムスタンプを得ることにより、複数の入力データについて同時にタイムスタンプを得ることができるという効果が得られる。

【0097】なおさらに、請求項5に係る発明によれば、送信手段で、電子署名生成手段で生成した電子署名を認証局に送信するので、入力データの認証をより確実に行うことができるという効果が得られる。なおさらに、請求項6に係る発明によれば、認証情報をハッシュ関数処理してハッシュ値を算出するようにしているので、改竄の検出を容易に行うことができると共に、認証情報と入力データとを含む全体のハッシュ関数処理することにより算出した総合ハッシュ値に電子署名を付けてタイムスタンプを得るだけで、証拠としての信頼性を確保することができるという効果が得られる。

【0098】また、請求項7に係る発明によれば、時間情報を使用者による変更が不可能な第1の時間発生手段及び使用者による変更が可能な第2の時間発生手段で個別に発生することにより、両者の時刻差から人為的な時刻の改竄を検知することができるという効果が得られる。さらに、請求項8に係る発明によれば、例えば全球測位システム(GPS)等の現在位置測定手段で測定した現在位置情報を認証情報に含めることができるので、入力データの入力位置を正確に特定することができるという効果が得られる。

【0099】さらにまた、請求項9に係る発明によれば、時間情報及び現在位置情報のログ情報を格納することにより、入力データの入力順番や情報認証装置での入力データの入力を確認することができ、入力データや認証情報の改竄を検知することができるという効果が得られる。なおさらに、請求項10に係る発明によれば、所有者情報入力手段で、所有者名、入力データがデジタル画像データであるときに撮影条件などのメモ等の所有者情報を入力し、この所有者情報をハッシュ関数処理して

ハッシュ値を算出するので、検証時に入力データに関する情報を特定することができるという効果が得られる。

【0100】また、請求項11に係る発明によれば、耐タンパー装置で認証情報のハッシュ値を算出すると共に、算出したハッシュ値、他の認証情報及び入力データの全てに対する総合ハッシュ値を算出し、算出したハッシュ値、総合ハッシュ値を物理的なコピー防止機能を有する第1の記憶手段に記憶し、入力データを物理的なコピー防止機能を持たない第2の記憶手段に記憶することにより、耐タンパー装置内で記憶するハッシュ値が入力データの大きさにかかわらず一定であり、第1の記憶手段の記憶容量を抑制することができるという効果が得られる。

【0101】さらに、請求項12に係る発明によれば、時間情報をログ情報として第1の記憶装置に記憶するので、このログ情報から入力データの入力順序を特定することができ、特に時間情報として使用者の修正可能な時刻情報及び使用者の修正不可能な時刻情報の2つの時刻情報又は使用者の修正可能な時刻情報及び全球測位システム(GPS)の時刻情報の2つを使用することにより、時間情報の改竄をより確実に防止することができるという効果が得られる。

【0102】さらにまた、請求項13に係る発明によれば、第1の記憶手段に時間情報及び位置情報をログ情報として記憶するので、このログ情報から入力データの入力順序をより確実に特定することができるという効果が得られる。なおさらに、請求項14に係る発明によれば、1つ前のエントリーのハッシュ値もログ情報として記憶するので、ログ情報のエントリーによるハッシュチェーンを形成することができ、ハッシュチェーンの一方方向性によって少なくともログ情報のエントリーの前後関係を保証することが可能となり、検証時にはエントリーの連続性の検証も行うことから不正なエントリーを隠しこむことを防止することができるという効果が得られる。

【0103】また、請求項15に係る発明によれば、耐タンパー装置に設ける第1の記憶装置の記憶容量に制限がある場合に、記憶すべき情報にデジタル署名を施して外部に出力することにより、耐タンパー装置内で生成された正しいものであることを証明することができるという効果が得られる。さらに、請求項16に係る発明によれば、デジタルカメラに情報認証装置を設けることにより、撮影したデジタル画像情報の証拠能力を格段に向上させることができるという効果が得られる。

【図面の簡単な説明】

【図1】本発明の一実施形態を表す情報認証システム構成を示すブロック図である。

【図2】図1の情報処理装置34の構成を示すブロック図である。

【図3】演算処理部で実行する認証識別子演算処理を示

すフローチャートである。

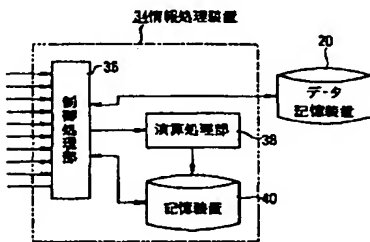
【図4】ハッシュ木を使用した場合における記憶数の説明に供する説明図である。

【符号の説明】

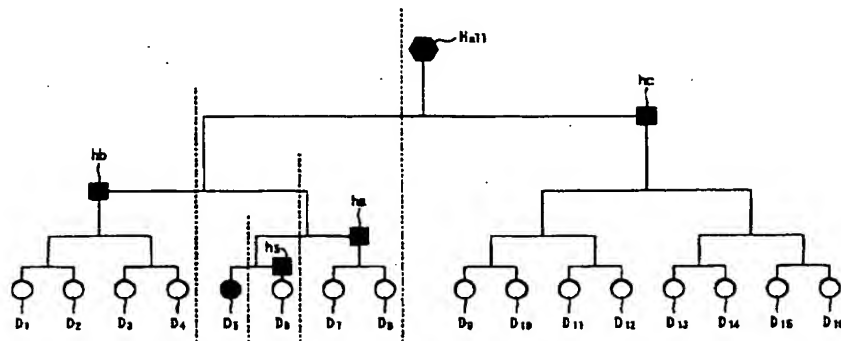
100 デジタルカメラ
200 タイムスタンプ生成機関
300 公開鍵認証機関
10 撮像部
12 個人情報入力装置
14 個人情報記憶装置
16 装置情報記憶装置

18, 50 通信装置
20 データ記憶装置
24 耐タンパー装置
26 第1の時刻情報発生装置
28 第2の時刻情報発生装置
30 位置測定装置
32 出力端子
34 情報処理装置
36 制御処理部
38 演算処理部
40 記憶装置

【図2】

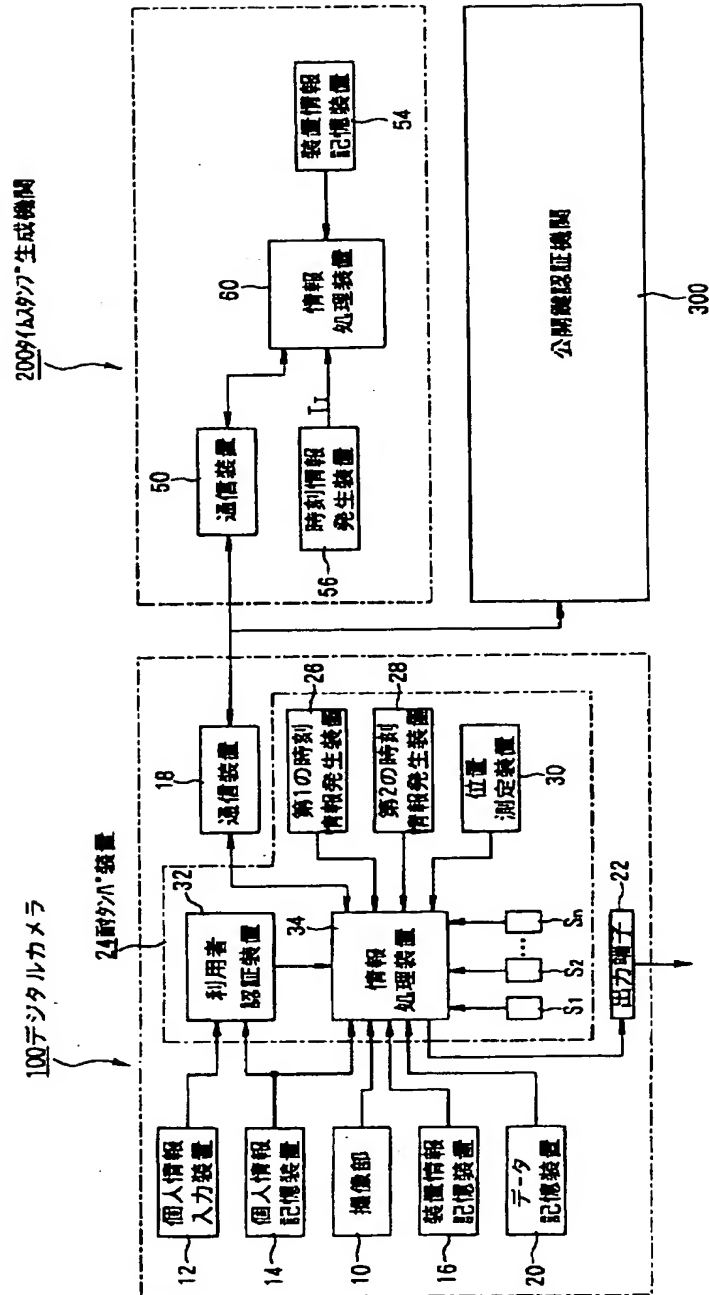


【図4】

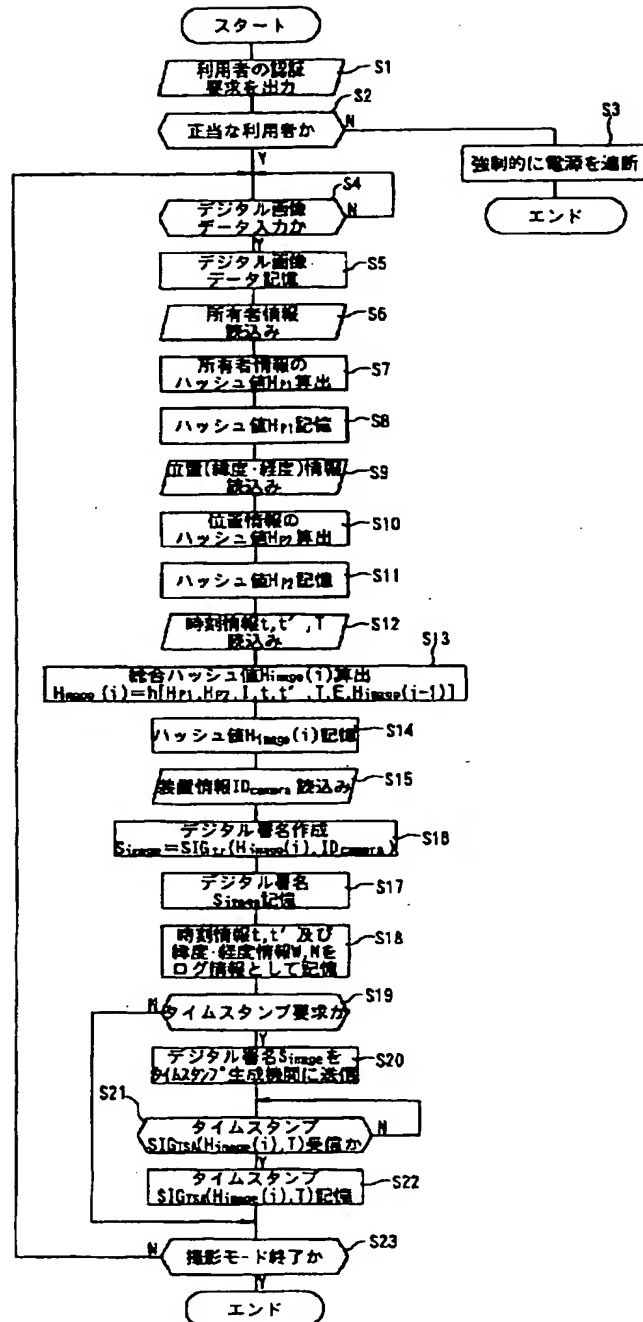


図：ハッシュ木

【図1】



【図3】



フロントページの続き

(72)発明者 古原 和邦
東京都三鷹市大沢 2-20-33 東京大学第
二武蔵野寮416

(72)発明者 今井 秀樹
神奈川県横浜市戸塚区品濃町557-44-205
Fターム(参考) SC022 AA13 AC69 AC75 CA00
SJ104 AA08 AA09 AA11 AA13 LA01
LA06 NA12